

AS



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,663	02/07/2002	Dongfeng Jing	08212/000S007-US0	3310

38879 7590 10/19/2005

DARBY & DARBY P.C.
P.O. BOX 5257
NEW YORK, NY 10150-6257

EXAMINER

POWERS, WILLIAM S

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	10/072,663		JING ET AL.	
	Examiner		Art Unit	
	William S. Powers		2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 February 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2/7/2002</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informality: In the specification the following description, "General Packet Radio Service Nodes (GGSNs) 125_{A-B}" (page 4, lines 14-15) refers to incorrect reference numbers.

Appropriate correction is required.

Claim Objections

2. Claims 1, 3, 5 and 8 are objected to because of the following informalities:

As to claim 1, improper articles are used in "a FA that..." (page 18, 3rd paragraph) and "a HA that..." (page 18, 6th paragraph) and "Diffie-Helman" (page 18, 4th paragraph) is misspelled.

As to claim 3, the verb "includes" (page 19, 1st paragraph) does not agree with the subject of that sentence.

As to claim 5, "Diffie-Helman" (page 19, 3rd paragraph) is misspelled.

As to claim 8, the word "fail" in the claim is in incorrect form.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 1-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As to claim 1, Applicant states "a[n] FA is configured to: ... authenticate, decrypt, sign and send the Reg-Reply message to the MN." (page 18, paragraph 3). There is no mention of encrypting the Reg-Reply message in the claim.

As to claims 2-12, they are rejected by virtue of their dependencies to claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2134

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-3 and 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 09/783,185 to Igarashi et al. (hereto referred to as Igarashi) in view of U.S. Patent Application No. 2002/0118674 to Faccin et al. (hereto referred to as Faccin) in further view of U.S. Patent No. 6,948,074 to Borella et al. (hereto referred to as Borella).

As to claims 1 and 13, Igarashi teaches a mobile IP system with:

- a. A mobile node that communicates with AAAH, AAAF, HA and FA nodes through registration-request and registration reply messages (page 11, paragraphs 227-230).
- b. An FA that communicates with the mobile node and the home agent (page 5, paragraphs 127-136 and page 11, paragraphs 227-230) and “decapsulates” [decrypts see page 8, paragraph 184] message packets (page 6, paragraph 154- page 7, paragraph 154).
- c. An AAAF and an AAAH, which are basically the same, that authenticates messages according to AAA protocol (page 6, paragraph 149). The AAAF generates session keys (page 13, paragraphs 267-269), adds identifiers and security information to registration request messages (page 9, paragraph 196).

- d. An HA that communicates with the AAAH with respect to registration request and registration reply messages (page 11, paragraphs 227-230).

Igarashi teaches the use of security protocols and measures (page 9, paragraph 196), but does not expressly mention the use of the Diffie-Hellman protocol or the signing of messages.

Faccin teaches the use of the Diffie-Hellman algorithm in determining session keys (page 3, paragraph 36) in order to maintain the security of the communication network between nodes.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the mobile IP system of Igarashi with the use of the Diffie-Hellman algorithm parameters for determining session keys of Faccin in order to maintain the security of the communication network between nodes.

Borella teaches messages signed in accordance with the X.509 protocol (column 10, lines 35-48) in order to provide authentication and ensure security of the messages.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the mobile IP system with Diffie-Hellman session keys of Igarashi and Faccin with the message signing of Borella in order to provide authentication and ensure security of the messages.

As to claim 2, Faccin teaches the use of Diffie-Hellman parameters to generate session keys (page 3, paragraphs 35-36) and signing of messages (page 4, paragraph 44).

As to claim 3, Igarashi teaches the use of NAI and session IDs to indicate the origin of messages (page 8, paragraphs 175-177).

As to claim 14, Faccin teaches the use of security associations to transmit, authenticate and authorize messages and keys in a secure manner between nodes (page 2, paragraph 30-page 3, paragraph 31).

As to claim 15, Faccin teaches the establishment of security associations between nodes in a mobile IP system (page 2, paragraph 29 and page 3, paragraph 37-page 4, paragraph 44).

6. Claims 4-12 and 16-20, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 09/783,185 to Igarashi et al. (hereto referred to as Igarashi) in view of U.S. Patent Application No. 2002/0118674 to Faccin et al. (hereto referred to as Faccin) in further view of U.S. Patent No. 6,948,074 to Borella et al. (hereto referred to as Borella) as applied to claims 1-3 above, and further in view of U.S. Patent Application No. 2002/0062385 to Dowling.

As to claim 4, Igarashi in view of Faccin teaches the use of security associations to transmit, authenticate and authorize messages and keys in a secure manner between nodes (Faccin page 2, paragraph 30-page 3, paragraph 31), but does not expressly mention the signing of messages by the security associations.

Dowling teaches security associations that digitally sign messages sent between nodes in order support security parameters and protocols (page 13, paragraph 116).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement mobile IP communication system of Igarashi, Faccin and Borella with the signing of messages by the security associations of Dowling in order support security parameters and protocols.

As to claim 5, Faccin teaches an AAAF that uses the Diffie-Hellman algorithm to generate session keys (page 3, paragraph 36).

As to claims 6 and 16, Dowling teaches the use of security association signatures to ensure authentication of messages (page 13, paragraph 116).

As to claim 7, Igarashi teaches the AAAF using identifiers in a Reg-Req message of an MN to find the AAAH of the MN (page 5, paragraphs 128-130).

As to claim 8, Igarashi teaches an AAAF that records the expiration time of a registration request/reply transaction (page 13, paragraphs 267-270).

As to claim 9, Dowling teaches a protection scheme against replay attacks (page 4, paragraph 43).

As to claim 10, Igarashi teaches a service profile that is created by the AAAH and securely distributed to the FA, HA and MN (page 8, paragraphs 173-176).

As to claim 11, Igarashi teaches using encapsulation [encryption] (page 8, paragraph 184) to securely transmit messages that include session keys between nodes (page 13, paragraphs 267-270).

As to claim 12, Igarashi teaches an HA that stores the current location of the MN as well as the session keys (page 6, paragraphs 150-153 and figure 12).

As to claim 16, Faccin and Dowling teach an authentic signature based on security associations, see claim 4 above. Igarashi further teaches the use of a service profile that includes session IDs in determining the authenticity of a message (page 5, paragraph 131).

As to claim 17, Faccin teaches the use of security associations to transmit, authenticate and authorize messages and keys in a secure manner between nodes (page 2, paragraph 30-page 3, paragraph 31). Dowling teaches security associations

that digitally sign messages sent between nodes in order support security parameters and protocols (page 13, paragraph 116).

As to claim 18, Faccin teaches an AAAF that uses the Diffie-Hellman algorithm to generate session keys (page 3, paragraph 36).

As to claim 19, Igarashi teaches a registration request message from a MN that includes a lifetime and authentication from an AAAH of the MN initiated by the FA (page 4, paragraph 126-page 5, paragraph 130). Faccin further teaches the use of Diffie-Hellman parameters to generate session keys (page 3, paragraphs 35-36), which are included in the registration request message.

As to claim 20, Igarashi teaches that the registration reply message includes the service profile of the MN (page 5, paragraph 131).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers, whose telephone number is (571) 272-8573. The examiner can normally be reached Monday-Thursday from 8 AM – 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
PO Box 1450
Alexandria, VA 22313-1450

Or faxed to:


(571) 273-8300

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (886) 217-9197 (toll-free).


WSP

October 6, 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 6100